SYSTEM AND METHOD FOR REMOTE OPENING OF HANDICAP ACCESS DOORS

BACKGROUND OF THE INVENTION

The present invention generally relates to systems and methods for the actuation of automatically opening handicap access doors.

Many public and private facilities are equipped with automatic door openers. Some open by detecting motion as someone approaches. Most public facilities require the pressing of a button mounted on a wall or post. An example of such a system is shown in Fig. 1. While these button-activated doors are functional, for some physically disabled individuals, the buttons are inconvenient and may be difficult to press depending upon the particular disability of the individual. For example, individuals with Cerebral Palsy may have great difficulty reaching and depressing the button. Quadriplegics generally cannot press these buttons at all. Blind individuals often have difficulty locating these buttons.

Another problem associated with button-actuated automatic doors is that they open very slowly to allow individuals with all types of disabilities to move from the button to the door before it begins to close. While this is effective to allow all individuals to effectively use the door, the slowness of the door opening may be frustrating to some disabled individuals who are capable of moving quickly towards the door. This problem is exasperated in cold and/or rainy weather.

SUMMARY

Accordingly, it is an aspect of the present invention to provide a mechanism for remotely activating an automatic door that does not require a user to press a preconfigured dedicated

button associated with the door. It is another aspect of the present invention to provide a system whereby the means for activating a door may be specially configured for each disabled individual so as to provide a mechanism that is the easiest to operate for that particular individual. Another aspect of the present invention is to enable such a system to open any public door as well as certain private doors. Still another aspect of the present invention is to provide an open standard that defines a wireless link for public access.

To achieve these and other aspects, features, and advantages, a control system for remotely activating an automatically opening door according to the present invention comprises: a plurality of transmitters held by different people, each transmitter transmits control signals; a plurality of doors at least some of which being mounted in different buildings, each of the doors including an actuator for automatically opening and closing the door; and a receiver electrically coupled to the actuator for receiving control signals from the transmitters and activating the actuator to open the door in response to the receipt of the control signals. In this system, any one of the transmitters may be used to open any of the doors.

Another aspect of the present invention is to provide a receiver for an automatic door assembly having a door and an actuator coupled to the receiver for automatically opening and closing the door in response to an activation signal. The receiver of the present invention comprises: a receiver circuit for receiving a rolling code control signal from a remote transmitter and a control circuit coupled to the actuator and the receiver circuit, wherein the control circuit is configured to decrypt any received rolling code control signal using a specific public key and to determine whether any received consecutive hopping codes are decrypted that correspond to consecutive codes of a rolling code algorithm. The control circuit supplies the activation signal

to the actuator when any received consecutive hopping codes are decrypted that correspond to consecutive codes of the rolling code algorithm.

Another aspect of the present invention is to provide a transmitter for remotely activating an automatic door having a door, an actuator for automatically opening and closing the door in response to an activation signal, and a receiver coupled to the actuator for supplying the activation signal in response to the receipt of a rolling code control signal having consecutive hopping codes that correspond to consecutive codes of a rolling code algorithm. The transmitter of the present invention comprises: a transmitting circuit for transmitting control signals and a control circuit for generating and encrypting a rolling code control signal using a public key, the rolling code control signal including a plurality of consecutive hopping codes, the sequence of which is determined in accordance with the same rolling code algorithm used by the receiver.

These and other features, advantages, and objects of the present invention will be further understood and appreciated by those skilled in the art by reference to the following specification, claims, and appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings:

Fig. 1 is a perspective view of a conventional button-activated automatic door;

Fig. 2 is a perspective view of an automatic door opening system of the present invention;

Fig. 3 is an electrical circuit diagram in block form of the control system of the present invention;

Fig. 4 is a block diagram illustrating the manner in which an encryption key is created and stored during production within a transmitter of the present invention;

Fig. 5 is a block diagram illustrating the basic operation of the transmitter; and

Fig. 6 is a block diagram illustrating the basic operation of a receiver of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figs. 2 and 3 show the control system of the present invention. As illustrated, system 10 includes a transmitter 15 for transmitting a control signal A. System 10 further includes at least one automatic door assembly 20 including door 24 and an actuator 22 that, when activated, automatically opens and subsequently closes door 24. Automatic door assembly 20 further includes a receiver 25 electrically coupled to actuator 22 for receiving the control signal A from transmitter 15 and for activating actuator 22 in response to the control signal. As shown in Fig. 2, transmitter 15 may be mounted to a support structure 32 of a wheelchair 30, which has a pair of wheels 34 rotatably mounted to support structure 32. An activation mechanism 17 (Fig. 3), which is coupled to transmitter 15, may be mounted in any location on wheelchair 30 and may take any form so as to make it as easy as possible for the individual to actuate transmitter 15. Activation mechanism 17 may be a conveniently located pushbutton or toggle switch, or may be a mechanism of the type that may be activated by a quadriplegic's tongue. Mechanism 17 may also be a voice or sound activated structure.

As explained further below, an unlimited number of transmitters may all be used to open any of an unlimited number of different automatic doors that may be on many different buildings. More specifically, the present invention pertains to an open standard by which manufacturers of such systems may make the respective transmitters and automatic doors such that any one transmitter will operate any of the automatic doors. In this manner, a disabled person may use such a transmitter to open any door that is constructed under the open standard.

The security of facilities equipped with automatic doors that respond to the transmitted control signals is no different than the security of conventional systems. When the facility is locked, the receiver is disabled just as the buttons on the post are disabled.

Transmitter 15 and receiver 25 may have any conventional structure and may be an infrared (IR) or preferably a radio frequency (RF) transmitter/receiver. As shown in Fig. 3, such a transmitter 15 would generally include a transmitter circuit 18 and a transmitter control circuit 19. Similarly, receiver 25 would generally include a receiver circuit 27 and a receiver control circuit 29. As will be described further below, transmitter 15 may transmit a rolling or other encrypted code. Additionally, transmitter 15 may be a trainable transmitter that is capable of learning the characteristics of an RF signal including the RF carrier frequency and code transmitted from another transmitter. Examples of such trainable transmitters are disclosed in U.S. Patent Nos. 5,442,340; 5,479,155; 5,583,485; 5,614,885; 5,614,891; 5,619,190; 5,627,529; 5,646,701; 5,661,651; 5,661,804; 5,686,903; 5,699,054; 5,699,055; 5,708,415; 5,903,226; and 5,854,593, the disclosures of which are incorporated by reference herein. U.S. Patent No. 5,661,804 discloses a trainable transmitter capable of learning rolling codes.

It will be appreciated by those skilled in the art that the transmitter could take the form of a transponder and the receiver could be a transceiver that transmits an interrogation signal and receives a reply signal from the transponder. In this manner, the transceiver could periodically transmit the interrogation signal and, when the transponder comes into range of the interrogation signal, and hence the door, the transponder responds to the interrogation signal by either modulating and transmitting the received interrogation signal or responding to the signal by transmitting a different control signal to which the transceiver responds by opening the door.

Actuator 22 and door 24 of automatic door assembly 20 may have any conventional structure since such conventional actuator structures are responsive to an electrical signal to open and close the door. In the case of the present invention, actuator 22 is responsive to an electrical signal originating from a receiver rather than a hardwired pushbutton of the type shown in Fig. 1.

By utilizing the system described above, the problems associated with prior art automatic doors are alleviated. Specifically, the automatic door may be modified to open more quickly so that individuals do not have to wait in the cold, rain or snow while the door opens. Moreover, because the door is not initially activated until the individual causes transmitter 15 to transmit the control signal, individuals that need more time to get to the door may wait and activate the transmitter when they are right next to the door. An additional advantage is that individuals may select the activation mechanism best suited for themselves given their particular disability.

Having generally described the structure of the system components, the radio link and data protocol of the present invention are described below.

The frequency of the transmission is preferably 433.92 MHz $\pm$ 25 kHz and the modulation shall be on-off-keyed (AM) modulation. The bandwidth (3dB) of the receivers is preferably $\leq$ 200 kHz. The minimum sensitivity of the receiver may also be specified. For example, the sensitivity may be defined as the lowest power delivered to a dipole, which successfully activates the receiver under the following conditions:

- 50 ohm RF source;
- vertical tuned dipole;
- 3 meter open field test site registered with the FCC; and
- receiver and dipole shall be mounted 1 meter above the ground.

Other testing conditions may be used for establishing such a minimum sensitivity standard.

The transmitters and receivers of the present invention preferably comprise encoders and decoders. In a preferred embodiment of the present invention, the encoders and decoders utilize hopping-code technology to provide a secure remote control system. Preferably, the encoders and decoders of the transmitters, receivers, transponders and/or transceivers used in the practice of the present invention comprise microchips which encrypt and decrypt the transmissions. For example, an encoder microchip of a transmitter of the present invention may comprise a circuit in which an identification number is stored, a circuit in which a counter value is stored, a logic circuit that changes the value of the counter value when the transmitter/encoder is operated, and a non-linear encoding circuit to encode the counter value to generate a transmission value which is decodable by a decoder microchip to provide the counter value. A decoder microchip of a receiver of the present invention may comprise a circuit in which a second identification number is stored, a circuit in which the transmission value from the encoder microchip is received, a circuit in which the transmission value is decoded to generate from the transmission value a decoded counter value, and a circuit in which a second decoded counter value obtained from a previous transmission value is stored. In addition, the decoder microchip may include a circuit in which signals are scanned to identify transmission signals conforming to a specific format. Encoders and decoders for use in the practice of the present invention as described above are available from Microchip Technology Incorporated ("Microchip") located in Chandler, Arizona. In addition, and in the alternative, encoders and decoders as described in U.S. Patent No. 6,175,312 titled "Encoder and Decoder Microchips and Remote Control Devices for Secure Unidirectional Communication" may be utilized in the practice of the present invention.

Preferably, the transmitters/receivers of the present invention include and utilize Microchip's HCS300 or HSC360 chip sets. The HSC300 and HSC360 devices are designed for

secure Remote Keyless Entry (RKE) systems. Both of these devices utilize Microchip's patented KEELOQ® hopping-code technology. The HSC300 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28-bit serial number and 6 status bits to create a 66-bit transmission stream. The HSC360 combines a 32-bit hopping code generated by a non-linear encryption algorithm, with a 28/32 bit serial number and 7/3 status bits to create a 67-bit transmission stream. The length of the respective transmission streams eliminates the threat of code scanning. The code hopping mechanism makes each transmission unique, thus rendering code capture and re-send (code-grabbing) schemes useless. The encryption keys, serial numbers, and configuration data are stored in EEPROM, which is not accessible via any external connection. The encryption keys and code combinations are programmable but read-protected. The HSC300 and HSC360 operate over wide voltage ranges of 2.0V to 6.3V, and 2.0V to 6.6V, respectively.

Preferably, each encoder, e.g., of a transmitter of the present invention, is programmed with the 28- or 32- bit serial number at the time of manufacture. This insures that each transmitter will be unique within a system. A 64-bit secret key is generated by a key generation function from the 28-bit or 32- bit serial number or a 32- or 48- bit seed and a 64-bit manufacturer's key as inputs. The generation of the secret key by using a key generation algorithm and the serial number and a 64-bit manufacturer's key as inputs is illustrated in Fig. 4. The manufacturer's key may be used to control the key generation function. The secret key is not readable and is never transmitted. The manufacturer's key/code is necessary in the receiver if a key generation function with a manufacturer's key/code was used to generate the secret keys. The manufacturer's key/code must be programmed into the receiver during manufacture. The manufacturer's key/code, according to the practice of the present invention, is generated and

fixed by the assignee of this invention or some other standard-establishing organization. The key generation function is used to generate a unique key for each transmitter from the serial number or a seed value. It is preferable that the function is non-linear. This function is performed by the programming station to generate keys to be programmed into transmitters. In normal learn mode, the receivers preferably use the same information that is transmitted during normal operation to derive the transmitter's secret key, decrypt a discrimination value and a synchronization counter. All of the transmitter information is then stored. The discrimination value is a 12-bit fixed portion of the encrypted word. It is preferred in the practice of the present invention that the discrimination bits are the least significant bits of the serial number. It is used as a post decryption check. As shown in Fig. 5, the synchronization counter is a 16-bit counter that is incremented on every activation of the encoder. It is stored on the receiver controller and compared to determine if a transmission is a previously received transmission, in which case it is ignored or if it falls within a forward window in which case it is accepted. In the practice of the present invention it is preferred to use the normal learn mode, that is, seed transmissions are not used. However, if a secure learn mode is used, the transmitter is activated through a special button combination to transmit a stored 32- or 48- bit value (seed) that can be used for key generation or be part of the key. Transmission of the random seed can be disabled after learning is completed. The seed is programmed into the encoder, preferably it is 32- or 48-bit. This can be programmed to be the same as one half of the key or can be used in key generation. The seed is only transmitted when a special button combination is activated and as stated, can be disabled once learning is complete.

It is preferred that the transmitter of the present invention transmit a 66/67-bit transmission format. The 66-bit transmission may be composed of a 32-bit encrypted string, a

28-bit fixed string, a 4-bit function code, a battery low indicator, and a repeat indicator. The 67-bit transmission may be composed of a 32-bit encrypted string, a 28- or 32-bit fixed string, 4- or 0- function code, battery low indicator, and a 2-bit CRC. The fixed string is the serial number of the encoder and remains constant for all transmissions from a particular transmitter. However, the 32-bit encrypted string is unique for each transmission. It is preferred in the practice of the present invention that a Long Guard function is enabled and every fourth transmitted word is blanked to lower the RF duty cycle. The Baud Rate is preferably 100 microseconds.

Before a transmitter can be used with a particular receiver, the transmitter must be "learned" by the receiver. Upon learning a transmitter, information is stored by the receiver so that it may track the transmitter, including the serial number of the transmitter, the current synchronization value for that transmitter, and the same encryption key that is used on the transmitter. In the proposed system, the receiver includes memory for storing a table in which anywhere between 500 and 1000 pairs of serial numbers and synchronization values are stored. Upon filling of the memory, the data pairs stored in the table may be purged on a first-in, first-out basis.

If the receiver receives a message of valid format, the discrimination bits are checked to verify the predetermined manufacturer's key. If the manufacturer's key is verified, then the serial number is checked and, if it is from a learned transmitter, the message is decrypted and the decrypted synchronization counter is checked against what is stored. If the synchronization value is verified not to exist in the table, or if the serial number does not exist in the table then the button status is checked to see what operation is needed. Typically, this will simply be a command to open and subsequently close a door. Nevertheless, various buttons may be

employed for performing different operations. Fig. 6 shows the relationship between some of the values stored by the receiver and the values received from the transmitter.

While the present invention contemplates very specific parameters for the purpose of establishing a standard, it will be appreciated that such parameters may be varied from those stated above so long as the same parameters are consistently used so that all receivers complying with the standard will respond to all the complying transmitters.

As will be appreciated by those skilled in the art, the transmitters could include additional activation mechanisms for performing other functions such as calling an elevator, turning on the lights in a home or office, or opening a private door.

The above description is considered that of the preferred embodiments only. Modifications of the invention will occur to those skilled in the art and to those who make or use the invention. Therefore, it is understood that the embodiments shown in the drawings and described above are merely for illustrative purposes and not intended to limit the scope of the invention, which is defined by the following claims as interpreted according to the principles of patent law, including the Doctrine of Equivalents.